

Notice of Allowability

Application No.

09/760,805

Examiner

Syed Zia

Applicant(s)

OBANA, SATOSHI

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to 01/04/2006.
2. ☒ The allowed claim(s) is/are 1-20.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

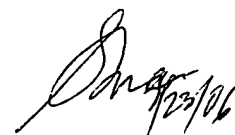
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____



DETAILED ACTION

Response to Amendment

This office action is in response to amendment and argument filed on January 04, 2006. Original application contained Claims 1-20. Applicant previously amended Claim 1, 7, 14, and 17-18. Therefore, presently Claims 1-20 are pending for consideration, and the Examiner's amendment is based on the previously recorded claims (dated July 18, 2005).

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Thomas A. Bilodeau (Reg. No: 43,438) on Thursday March 30, 2006.

This application has been amended as follows:

IN THE CLAIMS

Art Unit: 2131

Replace Claims 1, and 7 as follows:

Claim 1. A signature calculation system by use of a mobile agent, comprising:

a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent, wherein:

the base host includes:

an agent execution environment corresponding to the base host for letting the mobile agent execute its program code;

a random number generation means for generating random numbers;

a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means and a secret key of the owner of the mobile agent are inputted and which generates partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts; and

a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means, and

each remote host includes:

an agent execution environment corresponding to the remote host for letting the mobile agent execute its program code;

a partial signature calculation means to which signature target data, the signature

Art Unit: 2131

target data being target data to which a digital signature of the owner is to be attached, data which have been carried by the mobile agent including the partial signature auxiliary data, and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent;

a partial signature combining means to which one or more partial signatures calculated by one or more remote hosts are inputted and which outputs the digital signature calculated for the signature target data by use of the secret key of the owner of the mobile agent; and

a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature calculated by the partial signature calculation means, and

the mobile agent, which started from the base host carrying the partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the secret key of the owner of the mobile agent, and thereafter visits k (k : security parameter) remote hosts and carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the secret key of the owner of the mobile agent is obtained from the partial signatures calculated by the k remote hosts.

Claim 7. A signature calculation system by use of a mobile agent comprising: a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent

Art Unit: 2131

from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent, wherein:

the base host includes:

an agent execution environment corresponding to the base host for letting the mobile agent execute its program code;

a random number generation means for generating random numbers;

a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means are inputted and which generates a new secret key and a new public key corresponding to the newly generated secret key and generates partial signature auxiliary data for distributing the information of the newly generated secret key to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts, and generating a digital signature for the partial signature auxiliary data using a secret key of the owner of a mobile agent, and

a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means, and

each remote host includes:

an agent execution environment corresponding to the remote host for letting the mobile agent execute its program code;

a partial signature calculation means to which signature target data, the signature

Art Unit: 2131

target data being target data to which a digital signature of the owner is to be attached, data which have been carried by the mobile agent including the partial signature auxiliary data and a secret key of the remote host are inputted and which calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent;

a partial signature combining means to which one or more partial signatures calculated by one or more remote hosts are inputted and which outputs the digital signature calculated for the signature target data by use of the newly generated secret key; and

a public key cryptography calculation means for conducting encryption and signature calculation for the partial signature calculated by the partial signature calculation means, and

the mobile agent, which started from the base host carrying the partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the newly generated secret key, and thereafter visits k (k: security parameter) remote hosts and carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the newly generated secret key is obtained from the partial signatures calculated by the k remote hosts.

Response to Arguments

Applicant's arguments (specifically page 11-13) filed on January 04, 2006, with respect to Claims 1-20 have been fully considered and are persuasive. Therefore, the previous rejection has been withdrawn.

Allowable Subject Matter

1. Claims 1-20 are allowed.
2. The following is an Examiner's statement of reason for allowance:

The above mentioned claims are allowable over prior arts because the combined system of Cited Prior Art of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent Claims 1, 7, 13-14, 17-18, and subsequent dependent claims, when analyzed in light of specification.

In the system of cited prior arts Brickell discloses computing a signature (t, s), which is based on a number of individual values (ri) and (si) calculated by the individual RCA (Root Certification Authority) members based on individual keys of the RCA members. Brickell does not disclose a system with the *specific steps* of applicant's invention, including a base host and remote hosts, where the partial signatures are computed based on data input into the RCA members where that data falls into either category 1) signature target data, where the signature target data is target data to which a digital signature of the owner is to be attached, or 2) data which have been carried by a mobile agent including partial signature auxiliary data, where the partial signature auxiliary data is generated in the base host based in part on a secret key of the

Art Unit: 2131

mobile agent owner. Thus, the individual values (ri) and (si) of cited prior art are not calculated based on data falling into categories 1) or 2).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ

February 23, 2006

